



P/AU99/01051

REC'D 11 JAN 2000

WIPO PCT

AU99/1051

Patent Office
Canberra

I, KIM MARSHALL, MANAGER PATENT OPERATIONS hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PP 7283 for a patent by THE COMMONWEALTH OF AUSTRALIA filed on 25 November 1998.



WITNESS my hand this
Fourth day of January 2000

A handwritten signature in black ink, appearing to be 'K. Marshall'.

KIM MARSHALL
MANAGER PATENT OPERATIONS

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

This Page Blank (uspto)

THE COMMONWEALTH OF AUSTRALIA

ORIGINAL

AUSTRALIA
PATENTS ACT 1990

PROVISIONAL SPECIFICATION FOR THE INVENTION ENTITLED:

"HIGH ASSURANCE DIGITAL SIGNATURES"
This invention is described in the following statement:

This invention relates to digital signatures and in particular to high assurance digital signatures.

Background

5

Signatures are used by people in all aspects of everyday life. As society moves inexorably into the age of computers and information technology, the need for a signature which can be used in the digital realm is rapidly becoming a necessity.

10 Digital signatures however are not new and have been described in the research literature for nearly 20 years, but are not yet capable of being described as "commonplace".

15 However, as more security critical information is exchanged digitally, and more importantly the economic value of the information and transactions being handled digitally becomes more important, the need for a secure digital signature is likewise increasing in importance.

20 For the use of digital signatures to become readily accepted in high value or high-risk applications, it is necessary for them to be secure and there are a number of aspects to this security which are necessary precursors to their commonplace use in the future:

1. The cryptographic algorithms used to generate signatures have to be
25 complex enough to be unbreakable;
2. The users of the system need to have confidence in the public key distribution infrastructure;

3. The storage of private keys needs to be secure; and

4. The " endpoint" at which signatures are created and validated needs to be secure.

5

The literature describes numerous successful attacks against security measures taken to ensure the abovediscussed issues.

The invention described herein relates to the fourth aspect of security issues mentioned above, by seeking to provide a secure "endpoint" for creating and checking digital signatures.

Endpoint attacks

15 Endpoint attacks occur in the digital world and affect the act of creating or validating a digital signature and consequently this lowers the confidence of the recipients of digital messages that they are original or indeed originate from the purported sender of the message. An endpoint attack is different to that of a "protocol" attack which typically occurs during the transit of the message. In an
20 endpoint attack, the attacker typically alters software on a participants computer, to modify the messages which are being sent and received without the knowledge of the user, whereas in a protocol attack an attacker eavesdrops on communications between the respective computers, impersonating participants, or modifying missives, etc. and whereas there are suitable encryption techniques
25 to reduce or eliminate protocol attacks similar techniques have not been available to combat endpoint attacks in the critical area between the user and their own computer.

High assurance security

Technology for building secure systems has mostly been developed in the military intelligence communities. In high-risk situations, standards define high assurance systems. That is, the users or owners of systems have to be highly assured, or confident, that the software and hardware systems they use will perform correctly. The consequences of failure can be so significant, that it is justifiable spending substantial amounts of time and effort to achieve this assurance.

Assurance of this type is aimed partly at countering the threat of endpoint attacks and such assurance can be gained in a number of ways.

The most rigorous and objective methods, used by military intelligence organisations, are described in publications such as TCSEC, ITSEC, and CC. The majority of computers and computer systems however are not able to assure the reader or recipient of messages that the message has an acceptable level of assurance which would accord with that defined in the abovementioned publications.

Digital signature semantics

Signatures in the "paper" world are used to indicate that the person who signs the document has written or read and agreed with the content of the document. The term signature can also include a legal entity which may be represented in the form of a company seal applied by an authorised officer of the legal entity and typically countersigned by that person. Documents requiring signatures include, but are not restricted to, personal letters, contracts, or cheques.

It is important that, when digital signatures are used, they have the same legal value and effect as signatures used on a paper document. As with paper documents, if a digital document is signed by a person or a legal entity, the recipient and reader of the document should be able to assume that the signer
5 has written or at least read and agrees with the content of the document. However, in a digital world it is very easy to change digital documents without anyone knowing least likely but most importantly the signer of the document.

Assumed threats

10

To address this potential problem there are many computer systems today which can generate digital signatures for use with documents but which are still vulnerable to "endpoint" attacks. The designers and users of digital signing programs are often unaware of this type of threat but for those that are aware the
15 confidence or trust that a recipient can place in the fact that a statement was signed is never high and the whole system of digital signature and certificates is placed into jeopardy.

One manifestation of an endpoint threat is exemplified by a "Trojan horse" type
20 attack. A Trojan horse is a piece of malicious software, of which a user of the computer is typically unaware. The Trojan horse software as the name implies gains access to the memory of the computer being used, by accompanying a legitimate software program and once inside the computer, surreptitiously performs malicious functions, without knowledge of the user.

25

Consider a user who wants to sign an e-mail message. The private key may be kept encrypted in a file on the hard disc of the user's personal computer. To create the signature, the user must enter a password or phrase which allows the

file to be decrypted. The mail program can then perform the cryptographic calculations on the message to produce the signature using the private key.

5 It would be possible for the malicious program to read and then store the keys used by the user (in particular the key strokes that comprise the pass word or phrase) in another location on the hard disc, so as to enable the signing of other messages, which the user did not intend signing. For example, messages authorising the purchase and shipping of goods to a unknown recipient could be created and signed all without the authority or knowledge of the user. The
10 Trojan horse program may also secretly communicate the private keys of the user to another user, who could then fraudulently forge the user's digital signature on any document supposedly sent by the original user.

This is the primary threat eliminated or minimised by the present invention.

15

This invention provides high assurance digital signatures which can be embodied in a number of forms each of which is useful in different applications.

Specific embodiments of the invention will now be described in some further
20 detail with reference to and as illustrated in the accompanying figures. These embodiments are illustrative, and not meant to be restrictive of the scope of the invention. Suggestions and descriptions of other embodiments may be included but they may not be illustrated in the accompanying figures or alternatively features of the invention may be shown in the figures but not described in the
25 specification.

BRIEF DESCRIPTION OF THE FIGURES

Fig. 1 depicts a typical personal computer work-station and a high assurance digital signature device;

Fig. 2 depicts a pictorial representation of elements of the device;

Fig. 3 depicts a functional block diagram of the device; and

5

Fig. 4 depicts the use of a token with the device.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

- 10 In a preferred embodiment of the invention, refer Figure 1, a single chip processor with on-board ROM is used to implement the steps required to provide a high assurance digital signature. The device 10 in which this processor 12 and ROM 14 are embodied is located between the keyboard 16 and computer 18 and may also interface to the screen 20 of the computer. The more limited the
- 15 function of the of the microprocessor of the device the more it is amenable to high assurance evaluation which may be, in one embodiment, as is proscribed in the various documents mentioned previously, a well accepted level of trustworthiness as relevantly defined.
- 20 In a further preferred embodiment of the invention, refer Figure 2, a screen 22 is built into the device 10' itself, or the screen may be separated from the personal computer by a special switch 24 (refer Figure 3) which allows the user to be sure that what is being displayed on the screen is that which has been entered by the user or is under the control of the single chip processor device. The screen may
- 25 return to providing information provided by the user's personal computer or work-station after the physical review operation by the user signing the relevant digital information 26 (document) has been completed.

Yet in a further embodiment, refer Figure 3, of the invention, there is a trust mechanism 28 through which the user may indicate an acceptance or agreement with information displayed on the screen. This mechanism would typically involve the use of a button, or keypad. Alternatively, a predetermined keyboard switch could be used, so that at such times, the device "takes over" control, to receive instructions from the user. Therefore it is important that such an arrangement cannot be impersonated, say, by Trojan horse software which may exist on the personal computer, work-station or keyboard being used.

10 In a further embodiment, refer Figure 4, there is a method and means for storing a user's private keys. This may be in the form of a physical token 36, such as a Fortezza Crypto Card or smart-card. Or it may be a file on a remote computer server, however, such a file would need to be encrypted. This card can be inserted into the device 10 to be read by reader 32.

15 In yet a further embodiment a method for authenticating the user when a physical token is used for key storage would also provide a user authentication function such as biometric types of input mechanisms used to better identify the current user of the device.

20 In a further embodiment there is a means for performing the cryptographic algorithm to generate the signature which is built into the token containing the keys (providing an advantage that keys would never need to leave the token, thus increasing their security), or the method could use the dedicated processor
25 of the device to perform the encryption.

In a yet further embodiment there exists a mechanism for receiving the message from a computer, and for transmitting the signature (and possibly the message) to its next destination directly from the high assurance device. The physical

layer transport mechanism could be any type of standard computer interface, such as Ethernet, serial, parallel, PCI, SBus, SCSI, VSB, etc..

5 In one of the embodiments, the device would be able to perform with the signature generation function and the signal validation function. If it performs the signature validation function, it would need to be able to communicate the validity of the signature to the user in a trustworthy manner; ie. one which was not susceptible to forging by an untrusted agent. In one preferable approach, total control of the monitor is provided and an indicator on the device would
10 denote the information displayed on the monitor was trustworthy.

The message being signed may have an "indicator" within it, which is a type of security label and which if in existence provides a surety that the message was properly and authentically signed. The signature checker would, if a signature is
15 valid, and the indicator appropriate, output the message to the wider community. This approach could be used to implement a multilevel secure (MLS) messaging system refer to Figure 8.

In another embodiment the device would be programmed to produce signatures
20 in the format used by standard protocols, such as MSP,CSP (ACP-120),S/MIME,PGP, etc.. This would have the advantage that commercial off the shelf infrastructure used elsewhere would "understand" the signature, although it may not fully appreciate the high assurance nature of such signatures.

25 In some protocols, such as MSP, CSP, S/MIME, where there can be two signatures, the device can offer advantages over those mentioned above. The device can create one signature using the user's private keys, which may be used for purposes unrelated to the devices' invention. A second signature can be created using special keys devoted solely to the function of the invention.

This function may be useful for a user who has a Fortezza Crypto card or smart card and uses them for a number of different functions, only one of which is the generation of a high assurance digital signature. However, since the other
5 applications may be vulnerable to Trojan Horse attacks the recipient cannot have a high assurance in the digital signature information.

The device of the invention will be able to create the second signature, using special keys, to indicate the high assurance nature of the signature. Preferably,
10 the user's keys would be used to create an inner signature, which would be encompassed by the second signature created by, for example the Fortezza Crypto card, using the device's special keys.

A signature validating device may effectively translate the digital signature into
15 a conventional signature.

In financial institutions, many cheques are printed automatically, and in this embodiment, the device determines when the signature is valid, which would then allow information within the message to be printed on a cheque. The printer
20 will need to be connected directly to the device. Since the graphic containing the authorising (printed) signature is stored only within such devices, it can be assured that cheques appearing with the particular graphic could only have been produced with a high assurance digital signature device. Such a signature would be unique to the content of the cheque.

25

The high assurance digital signature device could be programmed to display information in particular formats which are in a convenient human readable form. For example, if messages are written in Hyper Text Markup Language

(HTML), the device could render the HTML, instead of showing all of the tags of the generated signature within the message.

5 High value electronic transactions may be required to be authorised using a high assurance device. The device would display Secure Electronic Transaction (SET) messages in a form convenient to the user.

10 The device of the invention is preferably able to check the authority of the user to sign certain types (eg. classifications) of messages, before proceeding to allow a user to do so. The user's authority could be stored with the keys, or in certificates communicated to the device with the message or at any other time.

15 The device of the invention is preferably able to encrypt information being transmitted, in order to preserve the confidentiality of the message content until it is decrypted by the recipient.

High assurance digital signature device

20 A preferred embodiment of the high assurance digital signature device comprises an embedded microprocessor which executes a program stored in ROM. Preferably the ROM and microprocessor are mounted on the same integrated circuit chip and arranged so that elements within the circuit cannot be changed so that the integrity of the device as created can not be interfered with.

25 Interfaces

In this preferred embodiment there are three operational interfaces:

Network Interface

In this embodiment the device contains an Ethernet network interface, and communications with the user's personal computer occurs over the Ethernet. The choice of this network protocol allows the device to be used with a wide
5 variety of personal computers, work-stations, X-terminals, and other networked computers.

In some environments, it may be possible to assume that all user's computers will have, for example, SCSI or bi-directional parallel interfaces. There is also no
10 reason that these could not be used for communication with the device.

User Interface

In a further embodiment interfaces to the user may be categorised as bulk or
15 Boolean inputs or outputs.

1. A Boolean output interface could be as simple as a light emitting diode (l.e.d.) Such an output only needs to indicate whether the bulk output interface is active or not. When the l.e.d. is lit, it may indicate that the device has taken
20 over the user's screen.

2. The preferred bulk input interface is the keyboard of the user's computer. In other trusted systems a keyboard switch has been used to divert the output data from the keyboard to a different destination. Similar technology is used in
25 this embodiment to divert the keystrokes to the device, instead of the user's computer. An alternative mechanism is to have a keypad or keyboard built into the device. The bulk input device is used for the entry of data, such as, personal identification (PIN) phrases.

3. The preferred bulk output interface is the monitor of the user's personal computer. Just as the keyboard switch described above is used to "takeover" the keyboard, a video switch is preferably used to allow the device to "takeover" the monitor. Any output displayed on the monitor by the device can be trusted to be the output provided from the bulk input interface. The user can tell whether the information on the monitor is that supplied from the device or not, by checking the status of the Boolean output which, for example, may be a light emitting diode (l.e.d.). A monitor may also be built into the device.

4. A preferred Boolean input device is a simple push button switch mounted on the device. With such a switch, the user can provide a positive indication to the device that the document being displayed on the bulk output interface is acceptable.

User's Fortezza Crypto card Interface

In one embodiment the user is able to insert their Fortezza Crypto card into the device. This allows the device to authenticate the user, by checking that the user has entered the correct PIN phrase for the Fortezza Crypto card, and it also provides a convenient secure storage for the user's private keys used for encrypting messages if need be.

Functions of the Device

25 In one embodiment the device can be arranged to provide a limited range of functions. Using the "client -- server" model, the device can be described as a server. Note that this does not imply that it is a large machine, located in a special room, and shared by many users at once. In this embodiment it means that the device does not initiate actions itself, it only responds to requests from

another system or device, which is for the purposes at hand referred to as a client.

The client, typically the user's personal computer, sends requests to the device.

- 5 After performing the appropriate function as determined by the request, the device sends a reply back to the client.

In a preferred embodiment a number of functions which could be offered by such a device include login; set personality; submission and delivery.

10

An important aspect of the submit function is the secure manner of the reviewing and signing operations conducted by the device. The device is arranged to make it impossible for the message to be modified between the reviewing and signing steps of the process but this does not imply that after reviewing the message the

- 15 signing function must occur.

Secure Messaging

- 20 The following is a description of an embodiment of the way in which a high assurance digital signature device and method of use can be integrated into an existing messaging system which uses the MSP (Message Security Protocol) and a Fortezza Crypto card. A similar approach could be used for systems using other protocols.

25 Existing system

The typical messaging system incorporating MSP performs the login and message submission processes as follows which is in accordance with MSP ICD.

Note that although the order of some steps is important, the precise order described herein is not the only valid process.

1. The user starts a Messaging User Agent (MUA) program, such as Netscape, Exchange, or Notes. As part of the start-up sequence, the user is required to login to the Fortezza Crypto card. The MUA program provides a pop up box, into which the user is asked to enter a PIN phrase. The PIN phrase is passed as an argument to the MSP_LOGIN call.
2. The MSP_LOGIN function passes the PIN Phrase to the Fortezza Crypto card, which verifies it, thus authenticating the user.
3. The MSP_LOGIN function instructs the Fortezza to provide a list of personalities, whose private keys are stored on the card.
4. The MSP_LOGIN function returns, passing the list of personalities as a result.
5. The MUA program displays the list of personalities to the user in another dialog box. The user is invited to select one of the personalities with whose key, messages will be signed, encrypted, or decryption.
6. The MUA program passes the selected personality as an argument to the MSP_SETPERSONALITY.
7. The MSP_SETPERSONALITY function instructs the Fortezza Crypto card to select the appropriate private key.

8. When the user chooses to send a new message the MUA program creates a window for the new message, and the user chooses a recipient/s (either by typing in addresses or choosing them from an address book), types in the message, and adds attachments if necessary. The user then selects the required security services: either none, sign, or sign and encrypt. When the composition is complete, the "Send" button is activated. The user's computer may or may not have control of the user's ability to attach certain files.

9. Submission access control then occurs.

10

10. The MUA program then begins the process of invoking none or "one or more" security options. For example, the Fortezza Crypto card is instructed by the MUA program to calculate a hash value (eg. MD5) and signature, and if appropriate, to encrypt the message. The signature and plain or encrypted message are constructed into a "Protocol Data Unit" (PDU) according to the protocol.

15

11. The PDU is attached to header or "envelope" information, which is then transferred to the messaging server, or Message Transfer Agent (MTA).

20

12. The typical delivery and verification/decrypted mechanism then follows.

Modifications to provide a high assurance mechanism

25 The following steps show the modifications required to change the existing system so that it can support the high assurance mechanism.

1. When the MUA is loaded, instead of loading in the standard MSP software as an integral part, software is loaded to allow the MUA to

communicate with the high assurance digital signature device. When the MUA calls the "MSP _ LOGIN" function, the software sends a signal to the device to indicate that the login function should commence. The device allows the user to enter the PIN phrase through a built-in keypad (or through the computer's keyboard, if keyboard switching functionality is included).

2. The device returns a signal to the computer, including the listed personalities. The software receives the signal, and "returns" the list as the result of the MSP _ LOGIN call. When the user chooses a personality, the MUA is loaded.

The high assurance digital signature mechanism preferably provides following features:

1. A message which is signed with a high assurance signature should not be vulnerable to Trojan horse software attacks on the computers of either the originator or receiver. That is, it is assumed that the software on all the systems have been maliciously changed to subvert the security of the computer.

2. Subject to the strength of the cryptographic algorithms it must be impossible to forge a high assurance signature.

3. The high assurance signature must be conveyed within standard protocols, thus allowing a user with Commercial Off the Shelf (COTS) standard compliant software to receive messages from, and transmit messages to, a user using the High Assurance Digital Signature device and method.

4. The user must be allowed to use their Fortezza Crypto card in an un-trusted computer for un-trusted applications.

In all the above embodiments the High Assurance Digital Signature is distributed from the device 10 via a network connection 11 (Fig. 1) or via the computer 18 and its network connection 13.

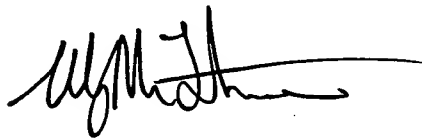
5

It will be appreciated by those skilled in the art, that the invention is not restricted in its use to the particular application described and neither is the present invention restricted in its preferred embodiment with regard to the particular elements and/or features described or depicted herein. It will be
10 appreciated that various modifications can be made without departing from the principles of the invention, therefore, the invention should be understood to include all such modifications within its scope.

15

Dated this 25th day of November, 1998.

THE COMMONWEALTH OF AUSTRALIA
By its Patent Attorneys
MADDERNS



20

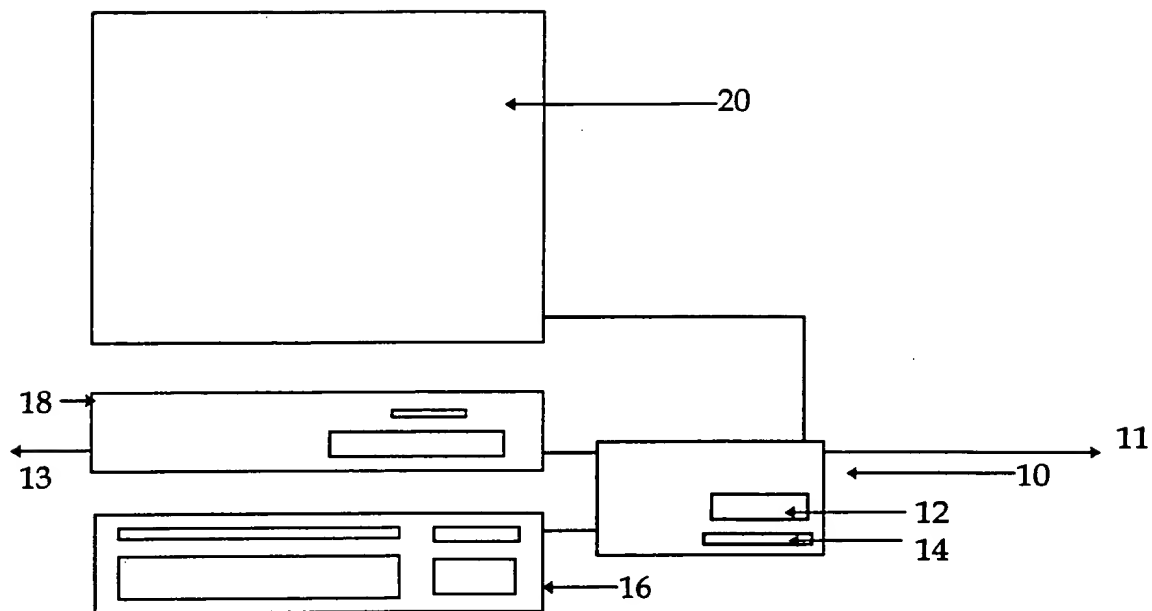


FIG. 1

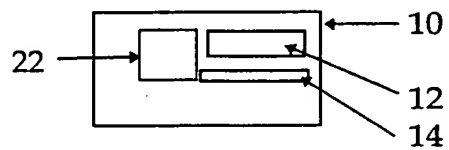


FIG. 2

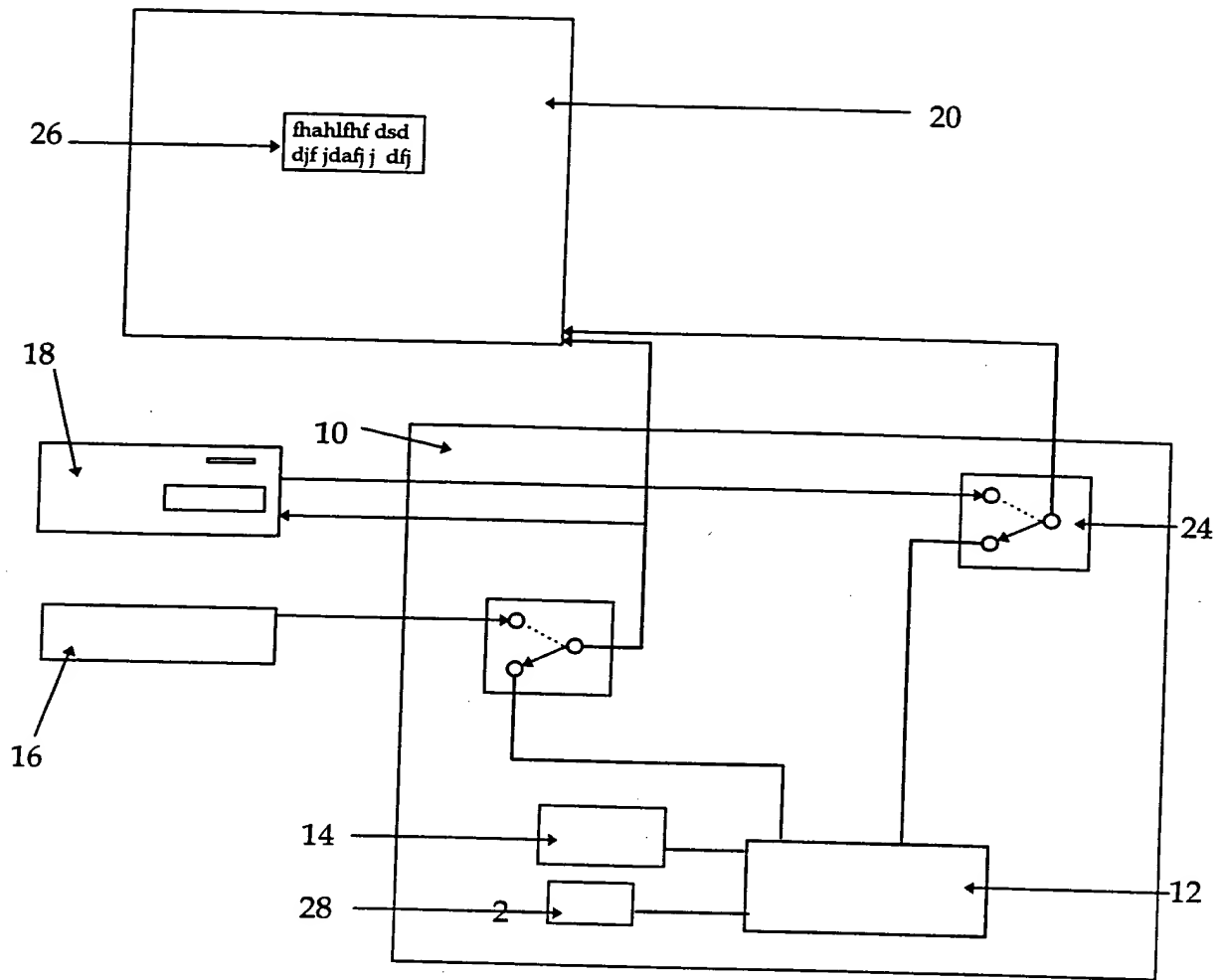


FIG. 3

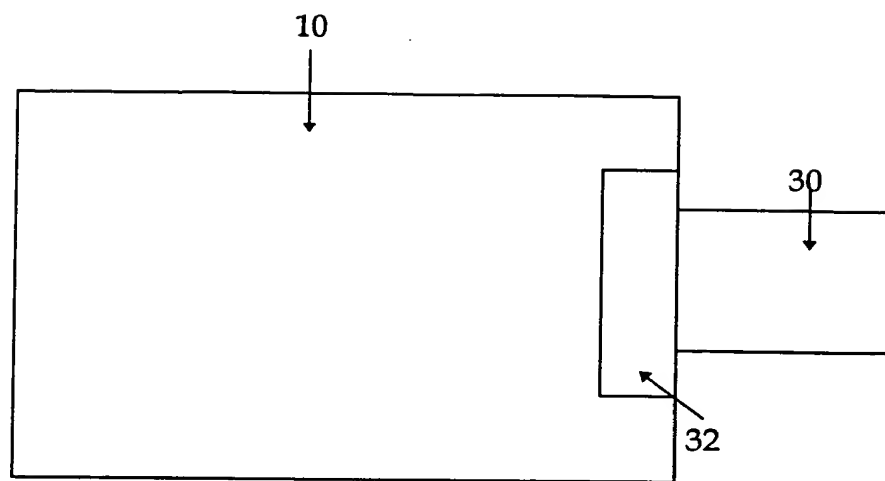


FIG. 4

This Page blank (uspto)